

Amendments to the Claims

1 Claim 1 (currently amended): A computer program product for efficiently generating pseudo-
2 random bits, the computer program product embodied on one or more computer readable media
3 and comprising:

4 computer-readable program code means for providing an input value; [[and]]

5 computer-readable program code means for generating an output sequence of pseudo-
6 random bits using the provided input value as input to a 1-way function, wherein a length in bits,
7 C, of the input value is substantially shorter than a length in bits, N, of the generated output
8 sequence; and

9 computer-readable program code means for using C selected bits of the generated output
10 sequence as the provided input value for a next iteration of the computer-readable program code
11 means for generating while using all N - C remaining bits of the generated output sequence as
12 pseudo-random output bits, until a desired number of pseudo-random output bits have been
13 generated.

1 Claim 2 (original): The computer program product according to Claim 1, wherein the 1-way
2 function is based upon an assumption known as "the discrete logarithm with short exponent"
3 assumption.

1 Claim 3 (original): The computer program product according to Claim 1, wherein the 1-way
2 function is modular exponentiation modulo a safe prime number.

1 Claim 4 (currently amended): The computer program product according to Claim 3, wherein the
2 input value is used as an exponent of the modular exponentiation.

1 Claim 5 (original): The computer program product according to Claim 3, wherein a base of the
2 modular exponentiation is a fixed generator value.

1 Claim 6 (original): The computer program product according to Claim 4, wherein the length of
2 the input value is 160 bits and a length of the safe prime number is 1024 bits.

1 Claim 7 (original): The computer program product according to Claim 1, wherein the length of
2 the input value is at least 160 bits and the length of the generated output sequence is at least 1024
3 bits.

Claim 8 (canceled)

1 Claim 9 (currently amended): The computer program product according to Claim [[8]] 1,
2 wherein the N - C remaining bits are concatenated to pseudo-random output bits previously
3 generated by the computer-readable program code means for generating further comprising:
4 —computer-readable program code means for concatenating bits of the generated next
5 sequential output sequence which are not selected by the computer-readable program code means
6 for selecting to the generated output sequence to form a longer output sequence of pseudo-
7 random bits.

1 Claim 10 (currently amended): The computer program product according to Claim [[8]] 1,
2 wherein the N - C remaining bits are selected from the N bits of the generated output sequence as
3 computer-readable program code means for selecting the subset of bits comprises selecting a
4 contiguous group of bits.

1 Claim 11 (currently amended): The computer program product according to Claim [[8]] 1,
2 wherein the N - C remaining bits are selected from the N bits of the generated output sequence
3 as computer-readable program code means for selecting the subset of bits comprises selecting a
4 non-contiguous group of bits.

1 Claim 12 (currently amended): The computer program product according to Claim [[8]] 1,
2 further comprising computer-readable program code means for using the desired number of
3 generated pseudo-random bits longer output sequence as input to an encryption operation.

1 Claim 13 (currently amended): A system for efficiently generating pseudo-random bits in a
2 computing environment, comprising:
3 means for providing an input value; [[and]]
4 means for generating an output sequence of pseudo-random bits using the provided input
5 value as input to a 1-way function, wherein a length in bits, C, of the input value is substantially
6 shorter than a length in bits, N, of the generated output sequence; and
7 means for using C selected bits of the generated output sequence as the provided input

8 value for a next iteration of the means for generating while using all N - C remaining bits of the
9 generated output sequence as pseudo-random output bits, until a desired number of pseudo-
10 random output bits have been generated.

1 Claim 14 (original): The system according to Claim 13, wherein the 1-way function is based
2 upon an assumption known as "the discrete logarithm with short exponent" assumption.

1 Claim 15 (original): The system according to Claim 13, wherein the 1-way function is modular
2 exponentiation modulo a safe prime number.

1 Claim 16 (currently amended): The system according to Claim 15, wherein the input value is
2 used as an exponent of the modular exponentiation.

1 Claim 17 (original): The system according to Claim 15, wherein a base of the modular
2 exponentiation is a fixed generator value.

1 Claim 18 (original): The system according to Claim 16, wherein the length of the input value is
2 160 bits and a length of the safe prime number is 1024 bits.

1 Claim 19 (original): The system according to Claim 13, wherein the length of the input value is
2 at least 160 bits and the length of the generated output sequence is at least 1024 bits.

Claim 20 (canceled)

1 Claim 21 (currently amended): The system according to Claim [[20]] 13, wherein the N - C
2 remaining bits are concatenated to pseudo-random output bits previously generated by the means
3 for generating further comprising:
4 —— means for concatenating bits of the generated next sequential output sequence which are
5 not selected by the means for selecting to the generated output sequence to form a longer output
6 sequence of pseudo-random bits.

1 Claim 22 (currently amended): The system according to Claim[[20]] 13, wherein the N - C
2 remaining bits are selected from the N bits of the generated output sequence as means for
3 selecting the subset of bits comprises selecting a contiguous group of bits.

1 Claim 23 (currently amended): The system according to Claim [[20]] 13, wherein the N - C
2 remaining bits are selected from the N bits of the generated output sequence as means for
3 selecting the subset of bits comprises selecting a non-contiguous group of bits.

1 Claim 24 (currently amended): The system according to Claim [[20]] 13, further comprising
2 means for using the desired number of generated pseudo-random output bits longer output
3 sequence as input to an encryption operation.

1 Claim 25 (currently amended): A method for efficiently generating pseudo-random bits,

2 comprising the steps of:

3 providing an input value; [[and]]

4 generating an output sequence of pseudo-random bits using the provided input value as
5 input to a 1-way function, wherein a length in bits, C, of the input value is substantially shorter
6 than a length in bits, N, of the generated output sequence; and

7 using C selected bits of the generated output sequence as the provided input value for a
8 next iteration of the generating step while using all N - C remaining bits of the generated output
9 sequence as pseudo-random output bits, until a desired number of pseudo-random output bits
10 have been generated.

1 Claim 26 (original): The method according to Claim 25, wherein the 1-way function is based
2 upon an assumption known as “the discrete logarithm with short exponent” assumption.

1 Claim 27 (original): The method according to Claim 25, wherein the 1-way function is modular
2 exponentiation modulo a safe prime number.

1 Claim 28 (currently amended): The method according to Claim 27, wherein the input value is
2 used as an exponent of the modular exponentiation.

1 Claim 29 (original): The method according to Claim 27, wherein a base of the modular
2 exponentiation is a fixed generator value.

1 **Claim 30 (original):** The method according to Claim 28, wherein the length of the input value is
2 at least 160 bits and a length of the safe prime number is at least 1024 bits.

1 **Claim 31 (original):** The method according to Claim 25, wherein the length of the input value is
2 160 bits and the length of the generated output sequence is 1024 bits.

1 **Claim 32 (original):** The method according to Claim 25, wherein the length of the input value is
2 at least 160 bits and the length of the generated output sequence is at least 1024 bits.

Claim 33 (canceled)

1 **Claim 34 (currently amended):** The method according to Claim [[33]] 25, wherein the N - C
2 remaining bits are concatenated to pseudo-random output bits previously generated by the
3 generating step further comprising the step of concatenating bits of the generated next sequential
4 output sequence which are not selected by the selecting step to the generated output sequence to
5 form a longer output sequence of pseudo-random bits.

1 **Claim 35 (currently amended):** The method according to Claim [[33]] 25, wherein the N - C
2 remaining bits are selected from the N bits of the generated output sequence as step of selecting
3 the subset of bits comprises selecting a contiguous group of bits.

1 **Claim 36 (currently amended):** The method according to Claim [[33]] 25, whercin the N - C

2 remaining bits are selected from the N bits of the generated output sequence as step of selecting
3 the subset of bits comprises selecting a non-contiguous group of bits.

1 Claim 37 (currently amended): The method according to Claim [[33]] 25, further comprising the
2 step of using the desired number of generated pseudo-random output bits longer output sequence
3 as input to an encryption operation.

Claim 38 (canceled)

1 Claim 39 (currently amended): An encryption system, comprising:
2 means for providing an input value;
3 means for generating an output sequence of pseudo-random bits using the provided input
4 value as input to a 1-way function, wherein a length in bits, C, of the input value is substantially
5 shorter than a length in bits, N, of the generated output sequence;
6 means for using C selected bits of the generated output sequence as the provided input
7 value for a next iteration of the means for generating while using all N - C remaining bits of the
8 generated output sequence as pseudo-random output bits, until a desired number of pseudo-
9 random output bits have been generated; and
10 means for using the desired number of generated pseudo-random bits of the generated
11 output sequence as input to an encryption operation.

1 Claim 40 (original): The encryption system according to Claim 39, wherein the 1-way function

2 is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

1 Claim 41 (original): The encryption system according to Claim 39, wherein the 1-way function
2 is modular exponentiation modulo a safe prime number.

1 Claim 42 (currently amended): The encryption system according to Claim 41, wherein the input
2 value is used as an exponent of the modular exponentiation.

1 Claim 43 (original): The encryption system according to Claim 41, wherein a base of the
2 modular exponentiation is a fixed generator value.

1 Claim 44 (original): The encryption system according to Claim 42, wherein the length of the
2 input value is 160 bits and a length of the safe prime number is 1024 bits.

1 Claim 45 (original): The encryption system according to Claim 39, wherein the length of the
2 input value is 160 bits and the length of the generated output sequence is 1024 bits.

Claim 46 (canceled)

1 Claim 47 (currently amended): The encryption system according to Claim 46, wherein the N - C
2 remaining bits are concatenated to pseudo-random output bits previously generated by the means
3 for generating further comprising:

4 ——means for concatenating bits of the generated next sequential output sequence which are
5 not selected by the means for selecting to the generated output sequence to form a longer output
6 sequence of pseudo-random bits; and
7 ——wherein the means for using bits of the generated output sequence as input to the
8 encryption operation further comprises means for using the longer output sequence as the input to
9 the encryption operation.